HITRUST CSF Requirements Included in Implemented, 1-year (i1) Assessments

As of Version 11.0.0 of the HITRUST CSF

CONFIDENTIAL & PROPRIETARY INFORMATION: The contents of this document are being provided to your organization for limited internal use only for the sole purpose of evaluating the HITRUST e1 assessment. This information cannot be shared outside of your organization, posted publicly, or used for any purpose other than evaluating the HITRUST e1 assessment. The contents of this document are confidential and proprietary and subject to copyright and intellectual property protection. The HITRUST CSF is owned by HITRUST Alliance, Inc., and any use of the HITRUST CSF, or components contained therein, are subject to the terms and conditions of the license agreement available at: https://hitrustalliance.net/product-tool/hitrust-csf/. This information is a small extract of the larger HITRUST CSF. The requirements included in the HITRUST e1 assessment may change over time; therefore, the content of this document may be outdated and should not be relied upon for readiness efforts. HITRUST reserves the right to make changes or updates to any of its assessments and/or the HITRUST CSF at any time.

Assessment Domain	Count of HITRUST CSF Requirements included in i1 Assessments
01 Information Protection Program	15
02 Endpoint Protection	7
03 Portable Media Security	6
04 Mobile Device Security	6
05 Wireless Security	7
06 Configuration Management	9
07 Vulnerability Management	12
08 Network Protection	9
09 Transmission Protection	9
10 Password Management	6
11 Access Control	21
12 Audit Logging & Monitoring	9
13 Education, Training & Awareness	6
14 Third-Party Assurance	8
15 Incident Management	7
16 Business Continuity & Disaster Recovery	10
17 Risk Management	10
18 Physical & Environmental Security	15
19 Data Protection & Privacy	10
	182

01 Information Protection Program

BUID	Requirement Statement
0101.00a1Organizational.123	The organization has a formal information security management program (ISMP) that is documented and addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP is based on an accepted industry framework, considers all the control objectives of the accepted industry framework, documents any excluded control objectives of the accepted industry framework and the reasons for their exclusion, and is updated at least annually or when there are significant changes in the environment.
0104.02a1Organizational.12	Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization's information security policies; protecting assets from unauthorized access, disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.
00109.02d1Organizational.4	Employees, contractors, and third-party users are: properly briefed on their information security roles and responsibilities prior to being granted access to covered and/or confidential information or information systems; provided with guidelines to state security expectations of their role within the organization; motivated and comply with the security policies of the organization; achieve a level of awareness on security relevant to their roles and responsibilities within the organization; conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and continue to have the skills and qualifications appropriate to their roles and responsibilities.
01109.02b1Organizational.7	The organization screens individuals requiring access to organizational information before authorizing access.
0113.04a1Organizational.2	The organization's information security policy is developed, published, disseminated, and implemented. The information security policy documents: state the purpose and scope of the policy; communicate management's commitment; describe management and workforce members' roles and responsibilities; and establish the organization's approach to managing information security.
0114.04b1Organizational.1	The information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Security policies are communicated throughout the organization.
0117.05a1Organizational.1	A senior-level information security official is appointed. The senior-level information security official is responsible for ensuring the organization's information security processes are in place, communicated to all stakeholders, and consider and address organizational requirements.
0126.05b1Organizational.1	Security activities (e.g., implementing controls, correcting nonconformities) are coordinated in advance and communicated across the entire organization where necessary.
0135.02f1Organizational.56	The organization's formal sanctions process: includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action; identifies the individual sanctioned; and identifies the reason for the sanction. The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures. The organization notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated.

BUID	Requirement Statement
0151.02c1Organizational.23	The organization ensures that employees, contractors, and third-party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization develops and documents access agreements for organizational systems. Privileges are not granted until the terms and conditions have been satisfied and agreements have been signed.
0173.05c1Organizational.45	The organization clearly allocates and assigns responsibilities to identify and protect individual IT assets in accordance with the security policies. Where necessary, the organization supplements policies with more detailed guidance for specific assets and facilities. When security responsibilities are delegated to others, the individual originally assigned these responsibilities remains accountable, and the organization determines that any delegated tasks have been correctly performed.
0180.05h1Organizational.4	An independent review of the information security management program and information security controls is conducted at least annually or whenever there is a material change to the business practices that may implicate the security or integrity of records containing personal information.
0181.06a1Organizational.12	All relevant statutory, regulatory, and contractual requirements, including the specific controls and individual responsibilities to meet these requirements, are explicitly defined and formally documented (e.g., in policies and procedures, as appropriate) for each information system type, and communicated to the user community as necessary through documented security training and awareness programs.
0183.07b1Organizational.1	All information systems are documented. Documentation of all information systems includes a method to determine accurately and readily the: assigned owner of responsibility; owner's contact information; and purpose (e.g., through labeling, coding, and/or inventory).
0193.09a1System.3	Operating procedures and the documented procedures for system activities are treated as formal documents. Changes to operating procedures and the documented procedures for system activities are authorized by management.

02 Endpoint Protection

BUID	Requirement Statement
0201.09j1Organizational.124	Technologies are implemented for the timely installation of anti-malware protective measures, timely upgrade of anti-malware protective measures, and regular updating anti-malware protective measures, automatically whenever updates are available. Periodic reviews/scans are required of the installed software and the data content of systems to identify and, where possible, remove any unauthorized software. The organization employs anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying a malicious code detection and repair software update, automated systems verify that each system has received its signature update. The checks carried out by the malicious code detection and repair software to scan computers and media include checking: any files on electronic or optical media, and files received over networks, for malicious code before use; and electronic mail attachments and downloads for malicious code before use or file types that are unnecessary for the organization's business before use; Web traffic, such as HTML, JavaScript, and HTTP, for malicious code; removable media (e.g., USB tokens and hard drives, CDs/DVDs, external serial advanced technology attachment devices) when inserted. The check of electronic mail attachments and downloads for malicious code is carried out at different places (e.g., at electronic mail servers, desktop computers, and when entering the network of the organization). Bring your own device (BYOD) users are required to use anti-malware software (where supported). Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.

BUID	Requirement Statement
0207.09j1Organizational.6	Centrally managed spam protection mechanisms are employed at information system entry and exit points, workstations, servers, and mobile computing devices on the network. Spam protection mechanisms detect and take action on unsolicited messages transported by electronic mail, transported by electronic mail attachments, transported by Web accesses, transported by other common means, and inserted through the exploitation of information system vulnerabilities. Malicious code and spam protection mechanisms are centrally managed and updated when new releases are made available in accordance with the organization's configuration management policy and procedures.
0210.01g1Organizational.1	All users are made aware of: the security requirements and procedures for protecting unattended equipment; their responsibilities for terminating active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver); their responsibilities for logging-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); and their responsibilities for securing PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use.
0217.09j1Organizational.7	The organization configures malicious code and spam protection mechanisms to: perform periodic scans of the information system according to organization guidelines; perform real-time scans of files from external sources at endpoints and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and block malicious code, quarantine malicious code, or send alerts to an administrator in response to malicious code detection.
0226.09k1Organizational.2	The organization implements and regularly updates mobile code protection, including anti-virus and anti-spyware.
0265.09m1Organizational.2	The organization applies a default-deny rule that drops all traffic via host-based firewalls or port filtering tools on its endpoints (workstations, servers, etc.), except those services and ports that are explicitly allowed.
02962.09j1Organizational.5	The organization augments endpoint protection strategies with additional solutions--including those built into the operating system if available--to mitigate exploitation of unknown vulnerabilities where traditional antivirus may be ineffective; and where applicable, target the solutions to protect commonly exploited applications (e.g., web browsers, office productivity suites, Java plugins).

03 Portable Media Security

BUID	Requirement Statement
0302.09o1Organizational.3	The organization protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography, tamper-evident packaging, a securable container (e.g., locked briefcase) via authorized personnel if hand-carried, and a trackable receipt by commercial carrier if shipped. The organization: maintains accountability for information system media during transport outside of controlled areas; documents activities associated with the transport of information system media; and restricts the activities associated with transport of such media to authorized personnel.
0304.09o1Organizational.2	The organization restricts the use of writable, removable media and personally owned, removable media in organizational systems.
0305.09q1Organizational.12	Media is labeled, encrypted, and handled according to its classification.
0311.09o1Organizational.5	Portable, removable storage devices are sanitized prior to connecting such devices to the information system under the following circumstances: initial use after purchase; when obtained from an unknown source; when the organization loses a positive chain of custody; and when the device was connected to a lower assurance system based on its security categorization (e.g., a publicly accessible kiosk).

BUID	Requirement Statement
0321.09u1Organizational.2	The organization protects physical media housing covered and/or confidential information from unauthorized disclosure or modification while in transit by the appropriate application of at least one of the following: use of locked containers; delivery by hand; tamper-evident packaging (which reveals any attempt to gain access); or splitting of the consignment into more than one delivery and dispatch by different routes.
0330.09o1Organizational.4	The organization limits the use of removable media to those with a valid business need. If such devices are required, the organization configures systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and automatically configures devices so that they automatically conduct an anti-malware scan of removable media when inserted or connected (e.g., through the use of third-party software).

04 Mobile Device Security

BUID	Requirement Statement
04.01x1Organizational.5	The organization identifies and encrypts mobile devices and mobile computing platforms that process, store, or transmit sensitive information.
0403.01x1Organizational.5	The organization monitors for unauthorized connections of mobile devices.
0404.01x1Organizational.5	Individuals are issued specifically configured mobile devices for travel to locations the organization deems to be of significant risk in accordance with organizational policies and procedures. Upon return from these locations the devices are checked for malware and physical tampering.
0407.01y1Organizational.4	Prior to authorizing teleworking: the physical security of the teleworking site is evaluated (e.g., of the building and local environment), and threats/issues associated with the physical security of the teleworking site are addressed.
0415.01y1Organizational.10	Suitable protection of the teleworking site is in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems, or misuse of facilities.
0429.01x1Organizational.5	The organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).

05 Wireless Security

BUID	Requirement Statement
0501.09m1Organizational.10	Prior to authorizing the implementation of wireless access points, the organization changes vendor default encryption keys, default SNMP community strings on wireless devices, default passwords/passphrases on access points, and other security-related wireless vendor defaults, if applicable.
0501.09m1Organizational.11	The organization changes wireless encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions.
0502.09m1Organizational.5	The organization ensures wireless access is explicitly approved and wireless access points and devices have appropriate (e.g., minimum of AES WPA2) encryption enabled for authentication and transmission.
0503.09m1Organizational.6	Wireless access points are placed in secure areas.
0504.09m1Organizational.13	Perimeter firewalls are implemented and configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the covered and/or confidential data environment.
0505.09m1Organizational.11	Quarterly scans are performed to identify unauthorized wireless access points. Appropriate action is taken if any unauthorized access points are discovered.

BUID	Requirement Statement
0506.09m1Organizational.12	Where a specific business need for wireless access has been identified, the organization configures wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, the organization disables wireless access in the hardware configuration (basic input/output system or extensible firmware interface).

06 Configuration Management

BUID	Requirement Statement
06.09b1System.2	Changes to information systems (including changes to applications, databases, configurations, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.
0601.06g1Organizational.124	Annual compliance assessments are conducted. Compliance reviews are conducted by security, privacy, and/or audit individuals, and incorporate reviews of documented evidence. If any non-compliance is found as a result of the review, managers will: determine the causes of the non-compliance; evaluate the need for actions to ensure that non-compliance does not recur; determine and implement appropriate corrective action; and review the corrective action taken.
0613.06h1Organizational.12	The organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools. If any non-compliance is found as a result of a technical security configuration compliance review, the organization: determines the causes of the non-compliance; evaluates the need for actions to ensure that non-compliance does not recur; determines and implements appropriate corrective action; and reviews the corrective action taken.
0627.10h1System.45	Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions. The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse.
0633.10j1System.1	Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) are strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes.
0636.10k1Organizational.3	The organization formally addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for configuration management.
0666.10h1System.5	The organization maintains an up-to-date list of authorized software that is required in the enterprise for any business purpose on any business system.
0667.10h1System.6	The organization is required to deploy application allow listing technology that allows systems to run software only if it is authorized to execute (allow listed) and prevents execution of all other software on the system in accordance with the allow list and rules authorizing the terms and conditions of software program usage.
06900.09d1System.2	The organization ensures separation between production and non-production (development, test/quality assurance) environments is established and controls are implemented to prevent operational issues.

07 Vulnerability Management

BUID	Requirement Statement
07.07a1Organizational.8	Organizational inventories of IT assets are periodically (annually at minimum) reviewed to ensure completeness and accuracy.

BUID	Requirement Statement
07.10m1Organizational.2	The organization deploys automated software update tools in order to ensure that systems are running the most recent security updates provided by the software vendor, and installs software updates manually for systems that do not support automated software updates.
07.10m1Organizational.3	Information systems are periodically scanned to proactively (annually at minimum) identify technical vulnerabilities.
0701.07a1Organizational.7	The organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites). The organization documents the importance of these inventoried assets. The asset inventory includes: all systems connected to the network; the network devices themselves; desktops; servers; network equipment (routers, switches, firewalls, etc.); printers; storage area networks; Voice Over-IP telephones; multi-homed addresses; virtual addresses; mobile phones, regardless of whether they are attached to the organization's network; tablets, regardless of whether they are attached to the organization's network; laptops, regardless of whether they are attached to the organization's network; other portable electronic devices [i.e., other than mobile phones, tablets, and laptops] that store or process data, regardless of whether they are attached to the organization's network; and approved bring your own device (BYOD) equipment.
0701.07a1Organizational.8	The asset inventories include: type or classification of the asset; format of the asset; location of the asset; backup information of the asset; license information of the asset; a business value of the asset; and data on whether the device is a portable and/or personal device. The asset inventory record is used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department. The asset inventory records: the network addresses; the machine name(s); the purpose of each system; an asset owner responsible for each device; and the department associated with each device. The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned. Records of property assigned to employees is reviewed and updated annually.
0704.07a1Organizational.8	The organization creates, documents, and maintains a process and procedure to physically inventory capital assets (at least annually), physically inventory non-capital assets, reconcile IT asset inventory information on hand for capital assets, reconcile IT asset inventory information on hand for non-capital assets. Organizational inventories of IT assets are updated during installations, equipment removals, system changes.
0704.07a1Organizational.9	The asset inventory includes the: unique identifier and/or serial number of the IT asset; information system of which the component is a part; type of information system component (e.g., server, desktop, application); manufacturer/model information of the IT asset; operating system type and version/service pack level of the IT asset; presence of virtual machines; application software version/license information; physical location (e.g., building/room number) of the IT asset; logical location (e.g., IP address, position with the IS architecture) of the IT asset; Media access control (MAC) address of the IT asset; data ownership and custodian by position and role; operational status of the IT asset; primary and secondary administrators of the IT asset; and primary user of the IT asset.

BUID	Requirement Statement
0706.10b1System.2	The organization develops applications based on secure coding guidelines to prevent: common coding vulnerabilities in software development processes; injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.); buffer overflow (Validate buffer boundaries and truncate input strings); insecure cryptographic storage (Prevent cryptographic flaws); insecure communications (Properly encrypt all authenticated and sensitive communications); improper error handling (Do not leak information via error messages); broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user); cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.); improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users); cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers; and any other input-validation vulnerability listed in the OWASP Top 10.
0709.10m1Organizational.1	Once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Further, the organization performs the necessary actions to correct identified technical vulnerabilities in a timely manner.
0715.10m1Organizational.4	Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled. Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).
0732.09r1Organizational.3	The access list for system documentation is kept to a minimum and is authorized by the application owner.
0778.10m1Organizational.5	The organization regularly compares the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

08 Network Protection

BUID	Requirement Statement
08.09m1Organizational.8	The organization prevents enterprise assets from accessing known malicious addresses and domains on the Internet (for example by means of browser configurations, DNS sinkholing, and/or use of a subscription service) -- unless there is a clear, documented business need and the organization understands and accepts the associated risk.
0802.01i1Organizational.2	The organization: determines who is allowed to access which network and networked services; specifies the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system); at a minimum, manages all enterprise devices remotely logging into the internal network, with remote control of their configuration; at a minimum, manages all enterprise devices remotely logging into the internal network, with installed software; at a minimum, manages all enterprise devices remotely logging into the internal network, with patch levels; publishes minimum security standards for access to the enterprise network by third-party devices (e.g., subcontractors/vendors); performs a security scan before allowing access; identifies the ports necessary for business and provides the rationale--or identifies compensating controls implemented--for those protocols to be non-secure; identifies the services necessary for business and provides the rationale--or identifies compensating controls implemented--for those protocols to be non-secure; and identifies the similar applications (e.g., protocols) necessary for business and provides the rationale--or identifies compensating controls implemented--for those protocols to be non-secure.

BUID	Requirement Statement
0805.01m1Organizational.12	Security gateways (e.g., a firewall) are used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of: enforcing security policies, being configured to filter traffic between these domains, and blocking unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered and/or confidential information systems environment.
0814.01n1Organizational.12	Network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization restricts the ability of users to connect to the internal network in accordance with the access control policy and the requirements of its business applications.
0815.01o1Organizational.1	The organization ensures that security gateways (e.g., a firewall) are used to validate source and destination addresses at internal and external network control points. The organization designs and implements network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a disallow list, or applying lists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter. Internal directory services and internal IP addresses are protected and hidden from any external access. Requirements for network routing control are based on the access control policy.
0816.01w1System.1	The sensitivity of an application is explicitly identified, and documented by the application/system owner.
0820.01k1System.3	The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection. Network devices that require authentication mechanisms use shared information (e.g., MAC or IP address) to control remote network access and access control lists to control remote network access.
0825.09m1Organizational.14	Technical tools such as intrusion detection systems (IDS)/intrusion prevention systems (IPS) are implemented and operating at the network perimeter and key points within the network. Implemented and operating technical tools include IDS and IPDS deployed on the wireless side of the firewall (WIDS). The IDS/IPS is updated on a regular basis, including the engines, baselines and signatures.
0835.09n1Organizational.1	The ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored. The right to audit is agreed by management for each network service provider. The security arrangements necessary for particular network services' security features, service levels, and management requirements, are identified and documented.

09 Transmission Protection

BUID	Requirement Statement
09.09v1Organizational.7	The organization uses an email filtering solution to recognize and block suspicious emails and unnecessary file types before they reach employee inboxes.
0903.10f1Organizational.1	Encryption is used to protect covered and/or confidential information transported by mobile or removable media and across communication lines. Encryption procedures supporting the encryption policy address the required level of protection (e.g., the type and strength of the encryption algorithm required), and specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).
0905.10g1Organizational.12	All cryptographic keys are protected against modification, loss, and destruction. Secret/private keys, including split-keys, are protected against unauthorized disclosure. Equipment used to generate, store, and archive keys is physically protected.

BUID	Requirement Statement
0913.09s1Organizational.5	Formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered and/or confidential information during transmission over less trusted/open public networks. Valid encryption processes include: Transport Layer Security (TLS) 1.2 or later; IPSec VPNs: Gateway-To-Gateway Architecture; Host-To-Gateway Architecture; Host-To-Host Architecture; and TSL VPNs: SSL Portal VPN; SSL Tunnel VPN.
0931.09v1Organizational.8	The organization has implemented Sender Policy Framework (SPF) by deploying SPF records in DNS, enabled receiver-side verification in mail servers to lower the chance of spoofed email messages, implemented DomainKeys Identified Mail (DKIM) to allow receiving servers to verify that email messages actually came from the organization, and implemented Domain-based Message Authentication, Reporting and Conformance (DMARC) to tell receiving servers to either quarantine or reject emails from the organization that don't pass SPF or DKIM.
0936.09w1Organizational.1	A security baseline is documented and implemented for interconnected systems.
0939.09x1Organizational.2	A documented agreement is committed and maintained for electronic commerce arrangements between trading partners including the agreed terms of trading and details of authorization. Other agreements with information service and value added network providers are also required.
0945.09y1Organizational.3	Protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL).
0954.10d1System.1	The information system provides mechanisms to protect the authenticity of communications sessions.

10 Password Management

BUID	Requirement Statement
10.01d1System.10	Password policies applicable to the organization's information systems are documented and enforced through technical controls.
1003.01d1System.3	User identities are verified prior to performing password resets.
1011.01f1Organizational.1	The organization ensures users are made aware of the organization's password policies and requirements, are made aware to keep passwords confidential, avoid keeping a record (e.g., paper, software file, or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved, change passwords whenever there is any indication of possible system or password compromise, do not share individual user accounts or passwords, do not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks), do not use the same password for business and non-business purposes, and select quality passwords.
1013.01r1System.2	The password management system stores passwords in protected (e.g., encrypted or hashed) form, transmits passwords in protected (e.g., encrypted or hashed) form, stores password files separately from application system data, enforces a choice of quality passwords, enforces password changes, and maintains a record of previous user passwords and prevents re-use.
1023.01d1System.11	The organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts before deploying any new devices in a networked environment.
10902.01d1System.12	Authentication credentials are provided using a secure method.

11 Access Control

BUID	Requirement Statement
11.01e1System.2	The organization reviews all accounts (including user, privileged, system, shared, and seeded accounts), and privileges (e.g., user-to-role assignments, user-to-object assignments) periodically (annually at a minimum).

BUID	Requirement Statement
11.01p1System.5	A policy applicable to the organization's information systems addressing account lockout after consecutive unsuccessful login attempts is documented and enforced through technical controls.
11.01q1System.3	The organization requires multi-factor authentication for network and local access to privileged accounts.
11.01q1System.4	The organization requires multi-factor authentication for access to non-privileged accounts from remote networks (including accounts in Web applications and in remote access solutions such as VPNs).
1101.01a1Organizational.1245	Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels, and information classification). The policy further defines logical and physical access control rules and rights for each user or group of users are considered together and clearly defined in standard user access profiles (e.g., roles). The access control program takes into account security requirements of individual business applications and business units and ensures standard user access profiles for common jobs roles in the organization.
1105.09c1Organizational.2	Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.
1107.01b1System.2	Default and unnecessary accounts are removed, disabled, or otherwise secured.
11124.01s1System.2	The use of system utilities is controlled by implementing the following: implementing identification, authentication, and authorization procedures; segregating of system utilities from applications software; and limiting the of the use of system utilities to the minimum practical number of trusted, authorized users.
11131.01u1System.2	Connection time controls are implemented for sensitive computer applications, especially from high-risk locations (e.g., public, or external areas that are outside the organization's security management). Connection time controls include using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration), restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation, and re-authentication at timed intervals.
1114.01h1Organizational.123	Covered or critical business information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use. Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately. When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).
11143.02i1Organizational.3	The organization ensures logical and physical access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility, or employment.
11149.02g1Organizational.2	The organization has a documented termination checklist that identifies all the steps to be taken and assets to be collected.
11152.02h1Organizational.1	The termination process includes the return of all previously issued software in the termination process, all corporate documents in the termination process, all equipment in the termination process, and all other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media in the termination process.
1117.01j1Organizational.23	Remote access by vendors and business partners (e.g., for remote maintenance) is disabled unless specifically authorized by management. Remote access to business partner accounts (e.g., remote maintenance) is immediately deactivated after use.
11183.01c1System.3	System administrators only use accounts with privileged access when performing administrative duties and use a separate user account with standard user access rights when performing non-privileged activities.

BUID	Requirement Statement
11190.01t1System.2	Both bring your own device (BYOD) and company-owned devices are configured to require an automatic session time-out screen as enforced through technical means.
1123.01q1System.2	Each user ID in the information system (including non-privileged, privileged, seeded, and service accounts) is assigned to a specific, named individual to maintain accountability.
1129.01v1System.12	The requirements for controlling access to applications and application functions are addressed, such as, but not exclusive to: providing menus to control access to application system functions; controlling which data can be accessed by a particular user; controlling the access rights of users, e.g., read, write, delete and execute; controlling the access rights of other applications; limiting the information contained in outputs; and providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.
1143.01c1System.123	The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role--user or administrator, only when needed).
1151.01c1System.2	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users and tracks and monitors privileged role assignments.
1194.01l1Organizational.2	Ports, services, and applications installed on a computer or network systems, which are not specifically required for business functionality, are disabled or removed.

12 Audit Logging & Monitoring

BUID	Requirement Statement
1203.09aa1System.2	Audit records include a unique user ID, unique data subject ID, function performed, and date/time the event was performed.
12101.09ab1System.2	The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.
12148.06i1Organizational.1	The organization determines which of the following auditable events require auditing on a continuous basis in response to specific situations: User log-on and log-off (successful or unsuccessful); Configuration changes; Application alerts and error messages; All system administration activities; Modification of privileges and access; Account creation, modification, or deletion; Concurrent log on from different workstations; and Override of access control mechanisms.
1223.09ac1System.1	Access to audit trails / logs is safeguarded from unauthorized access and use.
1235.06j1Organizational.1	Access to information systems audit tools is protected to prevent any possible misuse or compromise.
1239.09aa1System.4	Retention policies for audit logs are specified by the organization and the audit logs are retained accordingly.
1270.09ad1System.12	The organization ensures that proper logging is enabled in order to audit administrator activities. The organization ensures system administrator logs and operator logs are reviewed on a regular basis.
1272.09ae1System.13	Faults reported by users or by system programs related to problems with information processing or communications systems are logged. Error logging is enabled if this system function is available.
1295.09af1System.2	The organization uses at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

13 Education, Training & Awareness

BUID	Requirement Statement
13.02e1Organizational.6	Dedicated phishing awareness training is developed as part of the organization's onboarding program, is documented and tracked, and includes the recognition and reporting of potential phishing attempts.
1304.02e1Organizational.7	The organization provides role-based security-related training, especially for personnel with significant security responsibilities (e.g., system administrators), prior to accessing the organization's information resources, when required by system or environment changes, when entering into a new position that requires additional role-specific training, and no less than annually thereafter.
1306.06e1Organizational.5	All employees and contractors are informed in writing that violations of the security policies will result in sanctions or disciplinary action.
1307.07c1Organizational.124	The organization establishes and makes readily available to all information system users a set of rules that describe their responsibilities and expected behavior with regard to information and information system usage. Acceptable use addresses rules for electronic mail and Internet usages and guidelines for the use of mobile devices, especially for the use outside the premises of the organization. The organization includes in the rules of behavior containing explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.
1308.09j1Organizational.5	The organization prohibits users from installing unauthorized software, including data and software from external networks, and disables any auto-run features which allow file execution without user authorization (such as when files are downloaded from the Internet or when removable media is inserted). Users are made aware and trained on requirements relating to prohibition of installing unauthorized software, including data and software from external networks.
13998.02e1Organizational.2	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, prior to accessing any system's information.

14 Third-Party Assurance

BUID	Requirement Statement
1403.05i1Organizational.67	Access granted to external parties is limited to the minimum necessary, limited in duration, and is revoked when no longer needed.
1408.09e1System.1	Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions (e.g., reliability, availability, and response times for the provision of services), security controls, and other aspects of services management (e.g., monitoring, auditing, impacts to the organization's resilience, and change management).
1411.09f1System.1	The organization ensures a periodic review of service-level agreements (SLAs) is conducted at least annually, and compared against the monitoring records.
1414.09g1System.1	The organization ensures that third-party organizations use appropriate change management procedures for any changes to a third-party service or organizational system.
1416.10l1Organizational.1	Where software development is outsourced, formal contracts are in place to address: licensing arrangements; code ownership; intellectual property rights; certification of the quality and accuracy of the work; rights of access for the audit of the quality and accuracy of work; escrow arrangements; quality and security functionality requirements for the developed code; and security testing and evaluation prior to installation.

BUID	Requirement Statement
1419.05j1Organizational.12	The following security term is addressed prior to giving customers access to any of the organization's assets: description of the product or service to be provided; the right to monitor, and revoke, any activity related to the organization's assets; the respective liabilities of the organization and the customer. It is ensured that the customer is aware of their obligations. It is ensured that the customer accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization's information and information assets.
1428.05k1Organizational.2	The organization identifies and mandates information security controls to specifically address supplier access to the organization's information and information assets.
1444.09t1Organizational.12	Exchange and data sharing agreements specify the minimum set of controls on responsibility, procedures, technical standards, and solutions. The exchange and data sharing agreements also specify organization policies including: classification policy for the sensitivity of the business information; management responsibilities for controlling and notifying transmission, dispatch, and receipt; procedures for notifying sender of transmission, dispatch, and receipt; procedures to ensure traceability and non-repudiation; minimum technical standards for packaging and transmission; courier identification standards; responsibilities and liabilities in the event of information security incidents, such as loss of data; use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; technical standards for recording and reading information and software; any special controls that may be required to protect covered items, including cryptographic keys; and escrow agreements.

15 Incident Management

BUID	Requirement Statement
1506.11a1Organizational.2	A point of contact is established for the reporting of information security events. It is ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. The organization also maintains a list of third-party contact information (e.g., the email addresses of their information security officers), which can be used to report a security incident.
1535.11b1Organizational.12	The organization has an easy-to-use, available, and widely accessible mechanism for all employees, contractors, and third-party users to report incident and event information, including violations of workforce rules of behavior and acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents.
1560.11d1Organizational.1	The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy.
1561.11c1Organizational.4	The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).
1563.11d1Organizational.2	The organization incorporates lessons learned from ongoing incident handling activities and industry developments into incident response procedures, and training and testing exercises. The organization implements the resulting changes to incident response procedures, training exercises, and testing exercises accordingly.
1569.11e1Organizational.12	The organization collects, retains, and presents evidence to support legal action (either civil or criminal) in accordance with the laws of the relevant jurisdiction(s).

BUID	Requirement Statement
1589.11c1Organizational.5	The organization tests and/or exercises its incident response capability regularly.

16 Business Continuity & Disaster Recovery

BUID	Requirement Statement
16.09l1Organizational.4	The organization maintains offline backups of data and systems.
1602.12c1Organizational.4567	Business continuity plans: identify the necessary capacity for information processing during contingency operations, e.g., during an information system disruption, compromise or failure; identify the necessary capacity for telecommunications during contingency operations; identify the necessary capacity for environmental support during contingency operations; identify the essential missions and business functions; identify the contingency requirements associated with essential missions and business functions; provide recovery objectives; provide restoration priorities; provide recovery and restoration metrics; address contingency roles; assign individuals to contingency responsibilities; and contain the contact information of individuals assigned to contingency responsibilities.
1611.09h1System.2	The organization has allocated sufficient storage capacity to reduce the likelihood of exceeding capacity and the impact on network infrastructure (e.g., bandwidth).
1616.09l1Organizational.16	Backup copies of information and software are made regularly at appropriate intervals in accordance with an agreed-upon backup policy, are made when equipment is moved (relocated), and are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy. Restoration procedures are tested regularly at appropriate intervals in accordance with an agreed-upon backup policy.
1617.09l1Organizational.23	A formal definition of the level of backup required for each system is defined and documented including the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory, and business requirements. The organization formally defines and documents how each system is completely restored from backup.
1618.09l1Organizational.45	Backups are stored in a physically secure remote location and at a sufficient distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls are in place for the backup copies.
1632.12a1Organizational.1	The organization: identifies all the assets involved in critical business processes; considers the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management; ensures the safety of personnel and the protection of information assets and organizational property; and formulates and documents business continuity plans addressing information security requirements in line with the agreed business continuity strategy.
1634.12b1Organizational.1	The organization identifies the critical business processes requiring business continuity.
1666.12d1Organizational.1235	The organization creates, at a minimum, one business continuity plan. The organization ensures each plan: has an owner; describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security; specifies the escalation plan; specifies the conditions for the escalation plan's activation; and specifies the individuals responsible for executing each component of the plan.
1677.12e1Organizational.6	Responsibility is assigned for regular reviews of at least a part of the business continuity plan at a minimum, annually.

17 Risk Management

BUID	Requirement Statement
1701.03a1Organizational.12345678	The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.
1704.03b1Organizational.12	The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and the results reviewed annually.
17126.03c1Organizational.2	The organization implements an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.
1734.03d1Organizational.2	The risk management process is integrated with the change management process.
1739.05d1Organizational.3	Management formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization -- but no less than three years.
1744.05f1Organizational.23	The organization includes key contacts including phone numbers and email addresses as part of its incident management and/or business continuity plan. The organization designates a point of contact to review the list at least annually to keep it current.
1749.05g1Organizational.1	Membership in organization-defined special interest groups or forums/services are considered as a means to: improve knowledge of best practices and stay up to date with relevant security information; ensure the understanding of the information security environment is current and complete (e.g., threat monitoring/intelligence services); receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; gain access to specialist information security advice; share and exchange information about new technologies, products, threats, or vulnerabilities; and provide suitable liaison points when dealing with information security incidents.
1767.07d1Organizational.2	The organization establishes a classification schema to differentiate between various levels of sensitivity and value. Information assets are classified according to their level of sensitivity as follows: Level 1: Low-sensitive information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal, or hard copy; Level 2: Sensitive information that may not to be protected from public disclosure but if made easily and readily available, the organization will follow its disclosure policies and procedures before providing this information to external parties; Level 3: Sensitive information intended for limited business use that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners; Level 4: Information that is deemed extremely sensitive and is intended for use by named individuals only. This information is typically exempt from public disclosure. Users of information systems will be notified and made aware when the data they are accessing contains PII.

18 Physical & Environmental Security

ID	HITRUST CSF Requirement Statement
1801.08b1Organizational.124	Visitor and third-party support access are recorded and supervised unless previously approved.
1803.08b1Organizational.5	Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained in accordance with the organization's retention policy.
1807.08b2Organizational.56	Visible identification that clearly identifies the individual is required to be worn by employees, visitors, contractors and third-parties.
18108.08j1Organizational.1	The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its equipment maintenance program (e.g., through policy, standards, guidelines, and procedures).
18109.08j1Organizational.4	The organization maintains a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
18110.08j1Organizational.5	The organization monitors and controls non-local maintenance and diagnostic activities; and prohibits non-local system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative."
18131.09p1Organizational.3	Disposal methods are commensurate with the sensitivity of the information contained on the media.
1814.08d1Organizational.12	Fire extinguishers and detectors are installed according to applicable laws and regulations.
1819.08j1Organizational.23	Maintenance and service are controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organization's maintenance program, taking into account whether this maintenance is performed by personnel on site or external to the organization.
1820.08j2Organizational.1	Covered information is cleared from equipment prior to maintenance unless explicitly authorized.
1823.08j3Organizational.12	Tools for maintenance are approved, controlled, monitored and periodically checked.
1824.08j3Organizational.3	Media containing diagnostic and test programs are checked for malicious code prior to use.
1825.08l1Organizational.12456	Electronic and physical media containing covered information is securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal.
1828.08a1Organizational.12	Computers that store or process covered information are located in rooms with doors and windows that are locked when unattended. External protection is considered for windows, particularly at ground level (public, sensitive, and restricted areas), and are not located in areas that are unattended and have unrestricted access by the public.
1830.08a2Organizational.1	Security perimeters, such as any boundaries where security controls are in place to protect assets from unauthorized access, are clearly defined, and the siting and strength of each of the perimeters depend on the security requirements of the assets within the perimeter (public, sensitive and restricted areas).
1845.08b1Organizational.7	For facilities where the information system resides, the organization enforces physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that the organization determines necessary for areas officially designated as publicly accessible.
1847.08b2Organizational.910	The organization ensures onsite personnel and visitor identification (e.g., badges) are revoked, updated when access requirements change, or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned, disabled or changed.

ID	HITRUST CSF Requirement Statement
1848.08b2Organizational.11	A restricted area, security room, or locked room is used to control access to areas containing covered information, and is controlled accordingly.
1876.08g1Organizational.2	Lightning protection is applied to all buildings, and lightning protection filters (e.g., surge protectors) are fitted to all incoming power and communications lines.
1877.08g1Organizational.3	Information assets handling covered information are positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage devices are secured to avoid unauthorized access.
1888.08h1Organizational.456	An uninterruptable power supply (UPS) is used for equipment supporting critical business operations to support orderly shutdown or continuous running (transition to long-term alternate power); UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations; and power contingency plans cover the action to be taken should the UPS fail.

19 Data Protection & Privacy

ID	HITRUST CSF Requirement Statement
1903.06d1Organizational.3456711	The confidentiality and integrity of covered information at rest is protected using an encryption method appropriate to the medium where it is stored; where the organization chooses not to encrypt covered information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO.
19142.06c1Organizational.8	Guidelines are issued by the organization on the ownership, classification, retention, storage, handling and disposal of all records and information.
19144.06c2Organizational.1	The organization has established a formal records document retention program.
19145.06c2Organizational.2	Specific controls for record storage, access, retention, and destruction have been implemented.
19180.09z2Organizational.12	The organization (i) designates individuals authorized to post information onto a publicly accessible information system, and (ii) trains these individuals to ensure that publicly accessible information does not contain nonpublic information.
19181.09z2Organizational.345	The organization (i) reviews the proposed content of information prior to posting onto the publicly accessible information system and on a recurring bi-weekly basis to ensure non-public information is not included, and (ii) removes nonpublic information if discovered.
19193.10c2System.34	Information system flaws are identified, documented, reported, and corrected.
19207.10i2System.2	Personnel developing and testing system code do not have access to production libraries.
19379.13fHIPAAOrganizational.4	The organization, acting as a covered entity, formally verifies with appropriate documentation, the identity and authority of persons (e.g., public officials) requesting PHI.
19441.13kHIPAAOrganizational.13	A covered entity or business associate may disclose PHI to a business associate and may allow a business associate to, receive, maintain, or transmit PHI on its behalf, if the covered entity or business associate obtains satisfactory, written assurance (e.g., a written contract, agreement or arrangement that satisfies the requirements of this control) that the business associate will appropriately safeguard the information.
19922.06fCMMCSystem.1	The organization employs cryptographic modules that are certified and that adhere to the minimum applicable standards when used to protect the confidentiality of information.
19980.06dHIPAAOrganizational.1	Workstations that can access electronic protected health information are configured with specifications that address: i) proper functions to be performed, ii) the manner in which those functions are to be performed, and iii) physical attributes of the surroundings.